EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with John R. King on 12/9/08.

2. The application has been amended as follows:

Claim 1

(Currently Amended) A method of transferring data over a computer network from a network server to a first client computer system, the method comprising:

receiving a request by a requestor using a first client computer system for data from at least one network server storing data, at least some of the data stored by the network server being encrypted;

verifying whether a public encryption key associated with the requestor is good;

if verification fails, requesting user input from the requestor and generating a public encryption key and a private encryption key based at least in part on the user input and based at least in part on an identification code associated with the first client computer system;

checking an attribute of the requested data stored on the network server to determine whether the requested data stored on the network server is encrypted with the public encryption key associated with the requestor;

if the attribute stored on the network server indicates that the requested data stored on the network server is encrypted with the public encryption key associated with the requestor, automatically sending the encrypted data to the first client computer system;

if the attribute stored on the network server indicates that the requested data is encrypted with a public encryption key that is different than the public encryption key associated with the requestor, automatically sending a message to the requestor indicating that the requested data is not encrypted with the public encryption key of the requestor;

if the attribute stored on the network server indicates that the requested data is unencrypted, encrypting the requested data stored on the server with the public encryption key associated with the requestor automatically and without user intervention to create encrypted data; and

sending the encrypted data to the first client computer system wherein the first client computer system automatically uses the private encryption key to decrypt the encrypted data without user intervention and sending the requested data to the first client computer system only if the requested data is encrypted and if the requestor is the owner of the encryption key.

Claim 5

(Currently Amended) A method of data storage and retrieval comprising:

verifying whether a public encryption key associated with the requestor is good;

if verification fails, requesting user input and automatically generating independently of information from a network server, a public encryption key and a corresponding private encryption key in a first client computer system based at least in part on the user input and based at least in part on an identification code associated with the first client computer system, wherein the network server stores at least some data in an encrypted format;

storing the public encryption key and the corresponding private encryption key in the first client computer system such that access to the private encryption key is limited solely to the first client computer system and wherein both the public and the private encryption keys are needed to decrypt encrypted data;

associating an attribute with a data file on the network server, the attribute indicating whether the data file is encrypted with the public encryption key associated with different requestors when stored on the network server, and the attribute indicating an owner of the public encryption key;

requesting the data file by a requestor from the network server using the first client computer system;

checking the attribute of the requested data file to determine whether the requested data file is encrypted with the public key of the requestor;

if the attribute stored on the network server indicates that the requested data is encrypted with a public encryption key that is not associated with the requestor, sending a message to the requestor indicating that the requested data is not encrypted with their key;

if the attribute stored on the network server indicates that the requested data file is encrypted with the public key associated with the requestor, forwarding the requested data file to the first client computer system; and

if the attribute stored on the network server indicates that the requested data file is unencrypted, sending the public encryption key from the first client computer system to the network server automatically and without user intervention;

forwarding the requested data file to the first client computer system after the public encryption key associated with the requestor is used to encrypt the requested data file to create an encrypted data file wherein the encrypted data file is forwarded to the requestor and sending the requested data file to the first client computer system if the requested data file is encrypted and the requestor is the owner of the public encryption key; and

automatically decrypting without user intervention storing the encrypted data file with the private encryption key on a storage medium in the first client computer system.

Claim 8

(Currently Amended) A computer readable data storage medium having stored thereon commands that are operative to cause a general purpose computer configured as a network server to perform a method of data retrieval comprising:

verifying whether an encryption key associated with a requestor is good;

if verification fails, requesting user input from the requestor and generating an encryption key based at least in part on the user input and based at least in part on an

identification code associated with the first client computer system;

receiving a request for a data file from a requestor using a first client computer system at a network server, wherein at least some data files are encrypted;

checking a file attribute of the requested data file stored on the network server to determine whether the requested data file is encrypted with the encryption key associated with the requestor, wherein the attribute is alterable by a network administrator;

if the file attribute stored on the network server indicates that the requested data file is encrypted with the encryption key associated with the requestor, routing the encrypted data file to the first client computer system if the requested data file is encrypted and the requestor is the owner of the encryption key;

if the file attribute stored on the network server indicates that the requested data file is encrypted with an encryption key that is different than the encryption key associated with the requestor, sending a message to the requestor indicating that the requested data is not encrypted with the encryption key associated with the requestor and;

if the file attribute stored on the network server indicates that the requested data file is unencrypted, automatically requesting the public encryption key associated with the requestor from the first client computer system;

automatically encrypting the requested data file using the public encryption key associated with the requestor to create an encrypted data file; and

routing the encrypted data file to the first client computer system if the requested

data file is encrypted and the requestor is the owner of the encryption key; and

automatically decryptinq without user intervention the encrypted data file with the private encryption key associated with the requestor.

Claim 12, 17 and 20 are cancelled.

Claim 24

(Currently Amended) The method of Claim 5, wherein the identification code is uniquely associated with hardware in the first client computer system.

Allowable Subject Matter

3. Claims 1, 5, 7-8, 13-14 and 21-24 are allowed.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Minh Dieu Nguyen/
Primary Examiner, Art Unit 2437